Before the

U.S. COPYRIGHT OFFICE, LIBRARY OF CONGRESS

In the matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies Under 17 U.S.C. 1201

Docket No. 2014-07

Response of Electronic Frontier Foundation to June 3, 2015 Copyright Office Questions on Proposed Class 21

1. Commenter Information:

Kit Walsh
Corynne McSherry
Mitch Stoltz
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
rulemaking-2015@eff.org

Counsel for EFF:
Marcia Hofmann
Law Office of Marcia Hofmann
25 Taylor Street
San Francisco, CA 94102
(415) 830-6664

1. Please explain whether the requested exemption would or could impact non-software copyrighted content that is offered through vehicle telemetry and/or entertainment systems. Could an exemption be crafted that would preserve protection of such content?

The proposed class is defined in terms of "vehicle software." Thanks to this definition, the exemption is already crafted to exclude entertainment products or any other non-software copyrighted content. Further, when media products are distributed with TPMs (as are DVDs or DRMed audio and video files and streams), circumventing the TPM on the media product would implicate Section 1201 *whether or not* an exemption applied to the act of circumventing the separate TPM on the vehicle ECU.

It is important that the vehicle software of telemetry and entertainment systems be accessible under the proposed exemption. Telemetry is a key source of information about a vehicle for use in repairs and aftermarket innovation.[1] And both telemetry and entertainment ECUs provide an avenue for users and third-party innovators to add new functionality relating to a vehicle's display or sound system (to present additional maintenance information or to make the interface less distracting, for example). The same is true where these ECUs control wireless communications interfaces (such as Bluetooth, WiFi, or 4G connections). Additionally, users who learn of vulnerabilities in the wireless communications interfaces[2] should be able to protect

[1] Clifford Atiyeh, *Automakers Agree to Fix Your Car Anywhere in "Right to Repair" Pledge*, Car and Driver (Jan. 29, 2014), http://blog.caranddriver.com/automakers-agree-to-fix-your-car-anywhere-in-right-to-repair-pledge/; EFF Comments of May 1, 2015, Appendix C, Statement of Thejo Kote ("Kote Statement") at ¶2.

[2] Dr. Charlie Miller & Chris Valasek, *Survey of Automotive Attack Surfaces,* at 15-20, http://illmatics.com/remote%20attack%20surfaces.pdf (describing vulnerabilities in wireless communications of vehicles, including specific discussions of Bluetooth, telematics, and Internet connections).

themselves by scanning the existing code to make sure it matches a known good configuration or by modifying their software to eliminate bugs, just as users routinely patch other computers to fix vulnerabilities. It would be dangerous to leave a legal cloud over law-abiding users' ability to secure these entry points into the vehicle's computer network, just as it would stifle innovation and user choice surrounding the vehicle aftermarket.

2. Please explain whether and/or how the purchaser of a used vehicle would be able to identify and assess modifications to vehicle software by the previous owner. What would be the process, as well as the cost and burden, of identifying such changes? What type of equipment would be necessary?

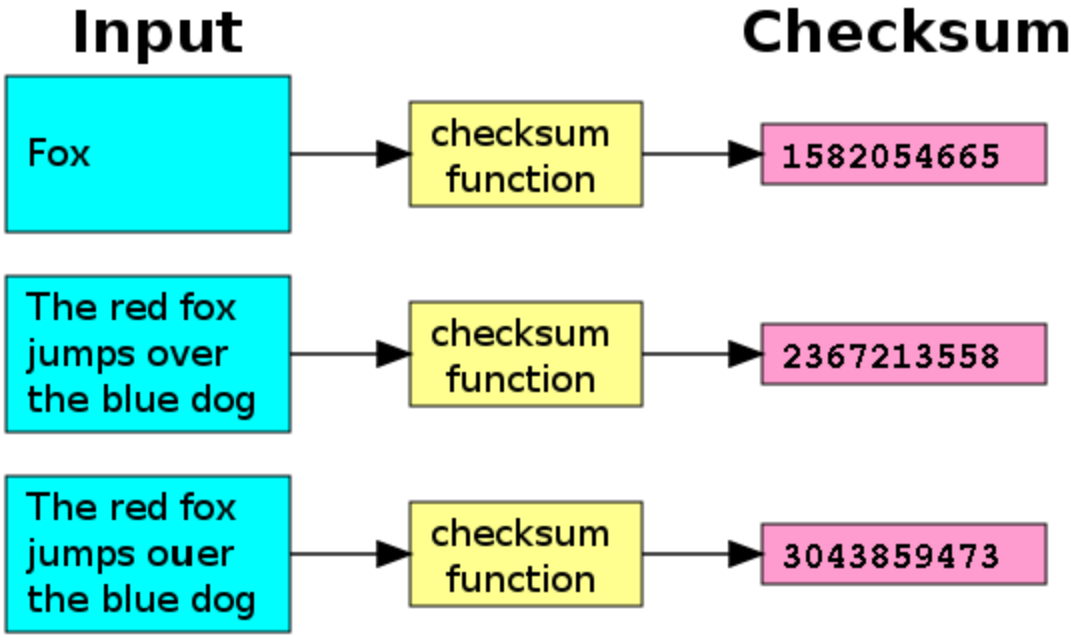
For a user who is able to access the vehicle software, verifying its integrity is quite easy. Programs are available for all major computer operating systems to evaluate a checksum (sometimes called a "hash sum") to verify that software has not been altered from a known configuration. NIST runs competitions to discover and evaluate new hash functions appropriate for government and private use in implementing checksums.[3]

The process of running a checksum simply involves feeding the code into a mathematical formula and confirming that the output matches what a trusted source says it ought to be. The chart on the following page[4] illustrates that even a small variation in the input results in a large and unpredictable change in the output. In order to overcome the security of a checksum, someone would have to write malicious code that evaluates to the same hash value (this is called a "hash collision") so that the change would not be detected by that particular algorithm. Properly implemented checksum algorithms make this computationally infeasible even for a determined attacker.[5]

[3] Chad Boutin, *NIST Selects Winner of Secure Hash Algorithm (SHA-3) Competition*, NIST Tech Beat (Oct. 2, 2012), http://www.nist.gov/itl/csd/sha-100212.cfm.

[4] Excerpt of Jorge Stolfi and Helix84, *Checksum.svg*, Wikipedia, (Nov. 22, 2008), https://en.wikipedia.org/wiki/File:Checksum.svg

[5] Shu-jen Chang, et al., *Third Round Report of the SHA-3 Cryptographic Hash Algorithm Competition*, NIST Interagency or Internal Reports 7896, at 9 (Nov. 2012), http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7896.pdf. This property is known as "collision resistance." *See id.* Even a weak, broken algorithm would detect changes to vehicle software made by someone who isn't intentionally trying to conceal what they are doing and would make it much, much harder to create altered software than to detect it.



No special preparation of vehicle software is needed for a checksum to verify its integrity. Nothing needs to be "installed" in the vehicle ECUs. And the algorithm is not a secret. It is simply a mathematical way of confirming that no alterations have been made to the software, by comparing it with the checksum of a known, trusted configuration.

Anyone could publish a list of checksums they endorse, from manufacturers to aftermarket innovators to members of a hobbyist community. A user might decide they trust one source but not others. The choice lies with the user.

Digital key-based signatures provide another, similar means of authenticating files. With PGP, for example, an author can create a digital signature for a file using their secret key (a data file – essentially just a very large, unique number).[6] Users who possess the corresponding public key can confirm that the digital signature must have come from the author. As the name suggests, the public key can be shared freely without compromising the security of the signature.[7] In this way, a key-based signature can be likened to a personalized checksum value. Just as generic checksums could be made available for known stable configurations of vehicle software, so, too, could key-based signatures from trustworthy sources.

Applications for verifying signatures and checksums are readily available: they are present by default on Linux and Apple desktop operating systems and are available for the other major operating systems as free and open source software.[8] There is no expense associated with these

---

[6] Callas, et al., *OpenPGP Message Format*, Internet Engineering Task Force, at 7, 76 (Nov. 2007), http://www.ietf.org/rfc/rfc4880.txt. *See also* Richard A. Mollin, *An Introduction to Cryptography* 227-240 (2nd ed. 2006).

[7] *Email Self-Defense*, Free Software Foundation, Inc., (last visited June 23, 2015), https://emailselfdefense.fsf.org/en/.

[8] *HowToMD5SUM*, Ubuntu Documentation, (July 12, 2014), https://help.ubuntu.com/community/HowToMD5SUM; *see GnuPG Download Page*, The GnuPG Project, (June 6, 2015), https://www.gnupg.org/download/.

tools. A user or their mechanic would simply need a hardware connection from their computer to the ECU, such as via the standard OBD port present in most vehicles, and would need to be able to read out the vehicle software. The cable to connect a laptop to an OBD port costs approximately ten dollars.[9] A mechanic able to access vehicle software would have negligible marginal cost in running a checksum.[10]

Given how remote the possibility is that such a check would be needed, it will likely be performed, at most, when first acquiring a used car or if a person has a particular reason to fear malicious activity or a malfunction in ECU memory. But it is simple enough that it could be routine if a need were demonstrated. For example, if security researchers reveal that a new attack is possible that modifies vehicle software, owners of potentially-affected vehicles could evaluate the checksums of their vehicle software to see if their vehicles have already been compromised, in addition to taking steps to eliminate their vulnerability.

At the hearing, one opponent asserted that their company has been working for years to implement a checksum system that does not even require the user to have access to the code itself. The requirement that the user *not have access* to the code is the difficult part of that process, not the checksum itself. Now that the project is apparently nearing completion, it will only make it easier for users to run checksums, assuming they choose to trust the manufacturer's claims about the integrity of the manufacturer's checksum system.

Well-known and freely available tools allow drivers and mechanics to verify that code on an ECU matches a known stable configuration. The obstacles to doing so are those imposed by manufacturers themselves and by the legal cloud of Section 1201.

3. The Office is interested in additional information concerning the costs and availability of manufacturing information and data to create diagnostic techniques and tools for the automobile "aftermarket," as well as the costs and availability of such information for persons who seek to create tools for individual use.

Some information that manufacturers use to develop aftermarket tools is not available on the open market. Manufacturers do not even claim that they provide all of this information to the market: the portion of the Memorandum of Understanding relating to aftermarket tools (Section 2(b)(ii)) commits only to providing "diagnostic repair information to each aftermarket scan tool company and each third party service information provider with whom the manufacturer has appropriate licensing, contractual or confidentiality agreements for the sole purpose of building aftermarket diagnostic tools and third party service information publications and systems." This means that the manufacturer can refuse to contract with any given aftermarket participant and has no obligation to sell them any information about how to communicate with vehicle ECUs. The agreement also does not even pay lip service to innovators who seek to improve on the functionality developed by manufacturers by using undocumented features of vehicle software or building aftermarket devices for purposes other than diagnosis and repair.

---

[9] *See, e.g.*, Car Diagnostics USB OBDII 409 Interface VAG-COM Cable, (last visited June 23, 2015), http://www.amazon.com/Diagnostics-OBDII-Interface-VAG-COM-Cable/dp/B008C3DC3Y/.

[10] Like other diagnostic, repair, and modification services, this service would not violate 1201(a)(2) because it would not provide the customer with access to the copyrighted work at all and thus cannot be characterized as a circumvention service. Even if it could, it does not meet the requirements of any of the three activities described in 1201(a)(2) for the reasons briefed by proponents. EFF Comments of February 6, 2015 at 24.

And, in fact, manufacturers do discriminate in terms of who is able to purchase which data about vehicle software. Nissan refused to sell data to Chris Valasek on the grounds that he was not an authorized dealer.[11] Mercedes has been criticized for considering transmission parts to be "theft relevant" and restricting needed information on that basis.[12]

Other vehicle software information is available only at great expense and is subject to anticompetitive contractual terms. Prices of up to $50,000 *per year* have been documented in the United States for the data stream license needed to develop aftermarket products, including diagnostics.[13] One individual complaining to NASTF about GM's licensing fees said he was quoted figures of $55,000 per year or $300,000.[14] He also reported that GM's policy meant that he could not deal directly with GM, but instead had to go through a company called SPX that has a subsidiary competing in the very market he sought to enter.[15] Healthy markets do not require a new entrant to gain an incumbent's permission to compete.

The contractual terms accompanying these licenses reportedly restrict licensees' ability to speak about the contract terms, restrict where licensees may sell their products, require that the license be maintained not only while the product is developed but for as long as the resulting product is sold, and require the licensee to pay *additional* fees and insurance costs.[16]

The ability to access vehicle software for reverse engineering is the only bargaining power that aftermarket participants have to get better terms from OEMs, and it is the only way that innovators can improve on OEMs' market offerings and compete on the merits of their innovation.[17] No one is saying that the OEMs may not ask a fair price for offering assistance to developers of aftermarket products; it is simply a matter of making sure they cannot abuse copyright law to create an effective monopoly on non-copyrightable information,[18] or to stifle the innovation of others. The more the legal cloud of Section 1201 seems to loom over access to vehicle software, the worse competition will fare and the fewer works of vehicle software will be authored. To vindicate the goals of copyright law and protect innovation, an exemption for the proposed class should be granted.

---

[11] Comment of Chris Valasek, June 2, 2015.

[12] *Sometimes, the dealership is the only option*, Fox 13 Tampa Bay, (May 6, 2013), http://www.myfoxtampabay.com/story/21576380/2013/03/11/sometimes-the-dealership-is-the-only-option.

[13] *Special OEM License Requirements*, The Equipment & Tool Institute TEK-NET Library, (last visited June 23, 2015), http://www.etools.org/OEMLicensing.

[14] *NASTF Information Requests,* National Automotive Service Task Force, (last visited June 23, 2015), http://www.nastf.org/custom/sir/report_detail.cfm?reportID=314.

[15] *Id.*

[16] *See Special OEM License Requirements*, *supra* note 13 (including examples of some such provisions, such as the requirement to purchase insurance). Unfortunately, the requirement of confidentiality in these contracts makes licensees understandably hesitant to come forward with their stories about the other common forms of restriction.

[17] Through reverse engineering, aftermarket companies can develop functionality that is not enabled by the commercially-available data or manufacturer tools. EFF Comments of May 1, 2015, Appendix A, Statement of David Thawley ("Thawley Statement") at ¶1.

[18] Manufacturers reportedly told Motor Magazine that the magazine could not write stories based on information published in factory "Technical Service Bulletins" without paying a licensing fee. Jim Thompson, *Right to repair*, Seacoastonline.com, (May 28, 2015), http://www.seacoastonline.com/article/20150528/NEWS/150529074/101179/OPINION.